Gartner Research

Decoding Vulnerability Management: A Stand Alone Tool vs. a Technique in Endpoint Protection

Jon Amato

24 March 2023

Gartner®

Decoding Vulnerability Management: A Stand-Alone Tool vs. a Technique in Endpoint Protection

Published 24 March 2023 - ID G00782165 - 13 min read

By Analyst(s): Jon Amato

Initiatives: Security Operations for Technical Professionals; Meet Daily Cybersecurity Needs

Vulnerability management capabilities are provided both by stand-alone VM platforms and as a feature by some prominent EPP platforms. Security and risk management technical professionals can use this research to select and use the right vulnerability management tool to satisfy their own needs.

Additional Perspectives

- Invest Implications: Decoding Vulnerability Management: A Stand-Alone Tool vs. a Technique in Endpoint Protection
  (29 March 2023)

Overview

Key Findings

- An increasing number of endpoint protection platform (EPP) tools are maturing to report on the vulnerabilities of the assets. The vulnerabilities reported are then prioritized and scored using risk-based prioritization techniques.
- Stand-alone vulnerability management (VM) tools and EPP tools with a VM technique use different scanning methodologies to discover vulnerabilities — stand-alone tools rely on periodic scans, while EPP tools use the continuous scanning or scanless methodology.
- Endpoint detection and response (EDR) tools with VM capabilities can potentially use vulnerability data to prioritize alerts and provide additional risk context to detection and response. These possibilities drive the inclusion of vulnerability management capabilities.

Recommendations

Security and risk management technical professionals focused on evaluating and selecting vulnerability management tools should:

- Compare core capabilities such as asset coverage, vulnerability signature coverage and supported integration features — that is, workflow tools, remediation tools or third-party prioritization technology — when selecting a vulnerability management product in order to satisfy their VM needs.
- Implement vulnerability management in a single tool whenever possible, to reduce complexity and operational overhead.
- Use the insights provided by the vulnerability management tool to better contextualize and prioritize EPP, EDR or XDR (extended detection and response) alerts.

Analysis

Vulnerability management is one of the most foundational tools in the enterprise security toolbox. However, approaches to VM have evolved over time. Over the more than 20-year life cycle of this technique, we have seen a shift from simply scanning and assessing the state of vulnerabilities, to managing and prioritizing their remediation.

One key change that has been observed in recent years is the inclusion of the vulnerability management functionality in enterprise toolsets where it has not traditionally been present; most prominently in endpoint protection platforms (EPPs).

There are, however, some significant differences between the way vulnerability management is done in the traditional vulnerability management toolset and the way it is implemented in endpoint protection tools (see Table 1).

Table 1: High-Level Comparison of Vulnerability Management Tools

Features	Stand-Alone VM Tool	EPP Tool With VM Technique
Scope of Coverage	Wide variety of assets, such as endpoints, network devices, Internet of Things (IoT) devices, cloud workloads, container environments, application scanning	Primarily Windows, Mac and Linux, with very limited support for other asset types
Deployment Architecture	Options are available for on-premises, cloud-hosted and hybrid implementations	Most EPP tools with vulnerability management only support cloud-based implementations
Scanning Technique	Agent-based and agentless scanning	Agent-based, with very limited support for network scanning
Vulnerability Signature	Broad signature coverage	Limited vulnerability signature coverage
Vulnerability Management Tool Ecosystem	Generally well supported by third-party tools for remediation, workflow and automated risk-based vulnerability prioritization	Minimal integrations with third-party remediation tools

Source: Gartner (March 2023)

Detailed Analysis

This section details how vulnerability management is approached in the different tools, as highlighted in Table 1.

Scope of Coverage

In this context, “Scope of Coverage” refers to the breadth of the assets that are covered in the vulnerability assessment capability of the tool.

Stand-Alone VM Tool

Stand-alone VM tools are the long-held standard for the detection of vulnerabilities in enterprise environments. Most tools in this space cover a wide variety of operating systems. At the baseline, they cover Windows, Mac and a variety of Linux distributions. Other, less commonly seen operating systems, such as AIX and HP-UX, also enjoy some degree of support.

In recent years, these tools have expanded coverage further into mobile platforms, IoT devices, cloud and container workloads, network infrastructure such as switches and routers, and even into network-connected storage appliances. Many of these tools support web application scanning and also include code scanning, such as dynamic or static application security testing (DAST/SAST). This enables them to provide the most complete coverage picture when assessing the organization's vulnerability posture.

EPP Tool With VM Technique

Typically, EPP tools are limited to the scope of support of the EPP tools themselves. The Windows operating system coverage is universal, with some EPP-based vulnerability scanners also covering Mac and Linux with limited support. In this type of tools, cloud and container support is uncommon, as is coverage for application vulnerabilities and code scanning.

Deployment Setup

Deployment setup varies for both tools. Generally, most vendors are moving toward cloud-based setup.

Stand-Alone VM Tool

As SaaS adoption in most enterprises grows rapidly, stand-alone VM tools have also started offering SaaS-delivered VM platforms. Easier management, less operational overhead and zero on-premises infrastructure requirements are the primary reasons why security professionals prefer SaaS over on-premises deployments.

However, some enterprises cannot send vulnerability information of their assets to third-party cloud services. Commonly, this is for regulatory reasons, but it is occasionally due to the local or regional business culture. For those organizations, many traditional VM vendors support an on-premises or a hybrid deployment setup, both using network-based and agent-based scanning techniques. This, in turn, helps the vendors to address the broadest set of customer requirements.

EPP Tool With VM Technique

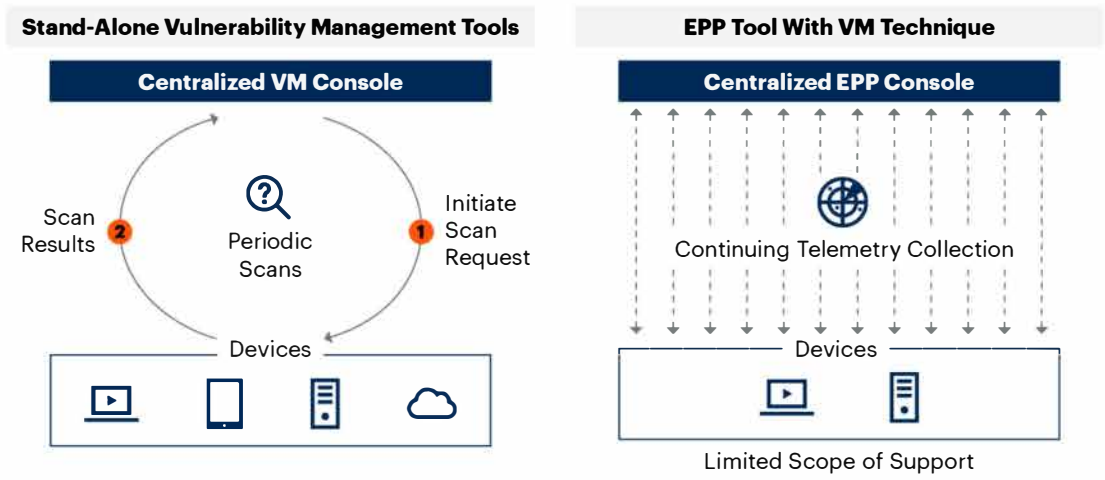
Most of the EPP vendors supporting vulnerability management features are delivered from the cloud. While many EPP tools still offer on-premises deployment, none of the tools offering the vulnerability management technique do so in their on-premises product versions at the time of this publication.

Scanning Methodology

Figures 1 and 2 illustrate the differences in scanning processes between stand-alone VM tools and EPP tools with the VM technique.

Download All Graphics in This Material

Figure 1: Comparison of Scanning Methodology



Source: Gartner
Note: EPP = endpoint protection platform; VM = vulnerability management
782165_C

Gartner

Scanning Technique

There are also some significant differences between the two toolsets in the methodology used for scanning for vulnerabilities.

Stand-Alone VM Tools

Stand-alone VM tools use a combination of local scanning by locally installed agents and network scanning. For most stand-alone VM tools, local agents can perform local discovery of vulnerabilities for which the VM tool has a signature. These local assessments commonly involve inspecting files, permissions and other configurations, such as Windows registry settings and other application configuration files.

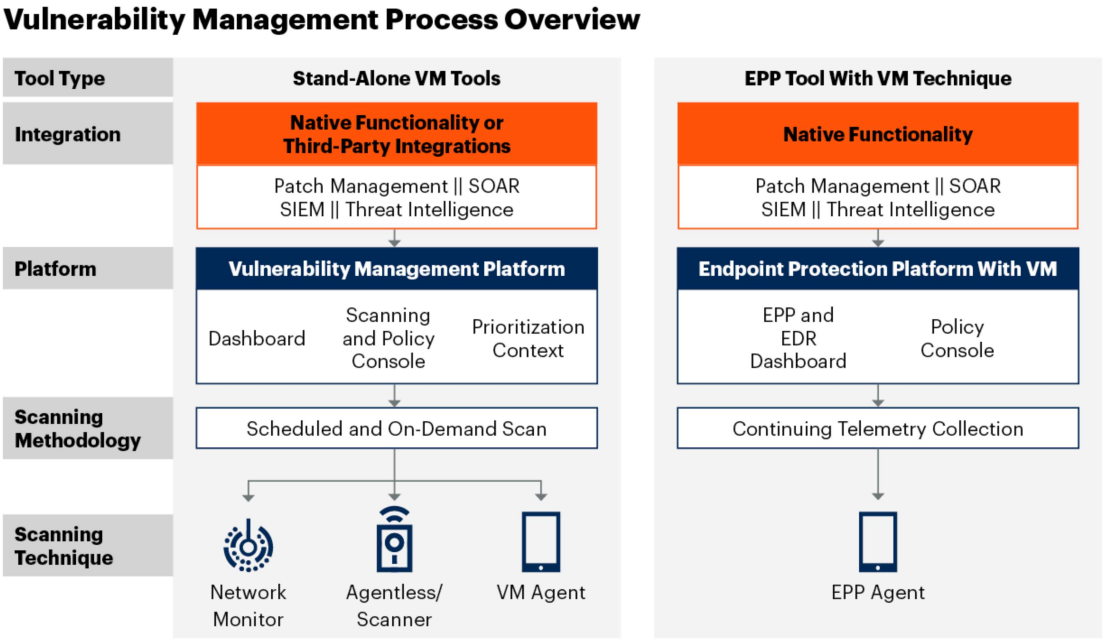
In addition, these tools have a network scanning capability to discover vulnerabilities in assets that may not have an agent present. They can also discover vulnerabilities in assets when there is no agent support for the operating system (OS) running on these devices. Network-based scans can use an authenticated scan technique, with previously configured credentials used to gain deeper visibility into the vulnerability posture of the scanned devices. Alternatively, they can be unauthenticated, meaning no credentials are used, but the level of scanning is more superficial.

EPP Tools With VM Technique

EPP tools with the vulnerability scan technique are, like traditional VM tools, primarily agent-based, using a local agent to provide deep visibility into the vulnerable operating system and application software present on a local machine. However, network scanning tends to be very limited, because scanned device support is often limited to a handful of network device types, such as a few popular storage and network infrastructure appliances.

The difference between the two scan methodologies can be illustrated in Figure 2.

Figure 2: Vulnerability Management Process Overview



Source: Gartner

Note: EDR = endpoint detection and response; EPP = endpoint protection platform; SIEM = security information and event management; SOAR = security orchestration, automation and response; VM = vulnerability management

782165_C

Gartner

Vulnerability Signature

At the heart of any vulnerability management tool is the signature set used for scanning — the actual intelligence that tells the vulnerability management tool what to look for. As with other aspects of these tools, there are some significant differences here as well.

Stand-Alone VM Tools

Owing to the long development history of these tools, the broadest vulnerability signature coverage is generally found here. Operating system vulnerabilities, even for older legacy OSes, are common, as are vulnerabilities in commonly used business software. Also, many vulnerabilities for which no patch exists can be detected here. In particular, these vulnerabilities result from misconfigurations, as opposed to actual software vulnerabilities. Further, web application vulnerabilities and other vulnerabilities not related to commercial off-the-shelf (COTS) software can also frequently be detected.

EPP Tools

With the VM technique found in EPP tools, vulnerability signature coverage tends to be more limited. Operating systems that are supported by the EPP agents themselves are able to be assessed, as are vulnerabilities found in the most common business software. However, configuration-related vulnerabilities are less commonly assessable. Vulnerabilities that have been mitigated — through closing ports, firewalls, NIPS, application control, behavioral monitoring or exploit protection — are likely to be incorrectly detected. This is because the agent-based assessment technique used extensively in EPP tools generally has fewer capabilities to detect mitigating and compensating controls that may be in place, and adjusts reporting to account for those controls.

Vulnerability Management Tool Ecosystem

Vulnerability management is a process, not just a tool. While identifying and reporting upon vulnerabilities found in the enterprise is the most common way vulnerability management tools are used, those are only two steps of that process. The ability to prioritize and remediate are as important as identification. To support this part of a mature enterprise vulnerability management program, a robust third-party tool ecosystem has emerged. However, there are some key differences between the ways these tools support traditional VM tools and EPP-type VM tools.

Stand-Alone VM Tools

When considering the vulnerability management third-party tool ecosystem, three categories of tools are most prominent: vulnerability prioritization, workflow management and automated remediation. In general, and owing to the overall maturity, traditional vulnerability management toolsets are well supported by this VM tool ecosystem.

EPP Tools

Generally speaking, and due to the rapid and recent emergence of EPP as a part of an enterprise vulnerability management program, endpoint protection-based VM is less well supported by these third-party tools that are so commonly used to support mature enterprise vulnerability management programs.

Recommendations

Choose a tool to fit your environment and meet your use cases. Remember, there is no one-size-fits-all recommendation for which tool is the right one for your organization. Based on the analysis and inquiry experience with Gartner clients, refer to the following table for scenarios that have been identified.

Table 2: Scenario-Based Selection

Scenario	Type of VM (Stand-Alone Tool or EPP With VM Technique)
You have no VM program in place and need to implement one — often resulting from compliance and regulatory reasons — but your EPP tool offers VM as a technique	Start with the VM technique in EPP, if that feature is available in your platform
You need to assess vulnerabilities on the broadest possible set of operating systems and devices	Prefer a stand-alone VM tool
You need a single consolidated view for application scanning and infrastructure vulnerability scanning	Prefer a stand-alone VM tool
Endpoints are already overwhelmed with a lot of agents	Opt for an EPP tool with a VM technique, or a stand-alone VM tool that supports agentless network scanning
You need third-party VM tool support — that is, prioritization, remediation, workflow	Prefer a stand-alone VM tool

Source: Gartner (March 2023)

If You Have No VM Program in Place, but Your EPP Tool Offers VM as a Technique

Although vulnerability management is one of the most foundational tools used in IT security programs, there are many organizations that are starting from a “greenfield” and have no incumbent vulnerability management tool. For those organizations, it may make sense to begin their vulnerability management journey with their endpoint protection product. Endpoint protection-based vulnerability management can give the organization the ability to assess the current state of the environment, develop operational processes around vulnerability management, begin the process of catching up with long-neglected vulnerabilities, and update the environment. Once the organization has developed more mature processes around vulnerability management, this decision could be revisited. With their requirements reevaluated, the organization could possibly “graduate” to a more mature, established vulnerability management tool.

You Need to Assess Vulnerabilities on the Broadest Possible Set of Operating Systems and Devices

Today's enterprise is not just about a single OS. Many modern IT infrastructures contain a wide variety of different operating systems and asset types ranging from mobile and laptops to cloud and container workloads — all of which must be accounted for in a well-implemented vulnerability management program. In order to cover this broad array of devices and software, the vulnerability tool used in mature VM programs must also have agent and vulnerability signature coverage for this broad array of devices. Endpoint protection-based VM tools generally do not support the breadth of operation systems and asset types, compared to those supported in a traditional vulnerability tool.

You Need a Single Consolidated View for Application Scanning and Infrastructure Vulnerability Scanning

The breadth of stand-alone vulnerability management tools extends past the array of devices and operating systems support. Application types and vulnerabilities in software are also in scope for a modern mature vulnerability management program, and the tools that support those programs need to support those as well. Techniques such as dynamic or static application security testing (DAST/SAST), infrastructure as code (IaC) scanning and container-at-rest scanning are important parts of the organization's overall vulnerability program. While there are specialist tools that can perform assessments of those types, many of the traditional vulnerability management tools can do those either natively or through a plug-in; all managed from the same console. On the contrary, EPP-based vulnerability management tools generally lack this functionality entirely. They require the use of these specialist tools, each with their own management interfaces and reporting. Additionally, they may need further manual report consolidation — often in tools like Excel — to support an overall top-down view of the vulnerability posture of the organization.

Endpoints Are Already Overwhelmed With a Lot of Agents

Every additional endpoint installed on an endpoint will inevitably consume additional system resources and ultimately impact the end-user-visible performance of the device. Furthermore, the ongoing chip shortage makes endpoint and server hardware harder to acquire. This requires many IT departments to "do more with less" and justify every additional byte of memory and CPU cycle dedicated to any security function, including vulnerability management. Since EPP-based vulnerability management tools reuse existing installed agents, the additional resource load will generally be lower than what can be expected when using the agent of a stand-alone VM tool. However, VM tools which can support network-based scanning generally consume far fewer system resources on the devices being scanned.

You Need Third-Party VM Tool Support

Vulnerability management tools are, in many enterprises that use them, only part of an ecosystem of tools used to manage vulnerabilities. This tool ecosystem includes:

- Tools used to remediate or patch discovered vulnerabilities.
- Tools used for risk-based prioritization of vulnerability mitigations.
- Workflow and ticketing systems.
- Configuration management and asset discovery systems.

These tools are all commonly integrated with vulnerability management tools. Integrations between these tools and vulnerability management tools are thus critical to efficiently manage vulnerabilities.

Well-established stand-alone vulnerability management tools, having been part of the IT security landscape for many years, tend to have better third-party tool integrations, to better fit into this overall ecosystem. However, EPP tools with VM capabilities are generally not as well supported in the third-party ecosystem of other auxiliary tools that commonly support programs of vulnerability management.

A Selection of Vulnerability Management Tools

Traditional stand-alone VM tools:

- Qualys
- Rapid7
- Tenable

EPP tools with VM capabilities:

- Crowdstrike Falcon Spotlight
- Microsoft Defender for Endpoint
- VMware Carbon Black Cloud Vulnerability Management
- SentinelOne

- Trend Micro Vision One
- Cisco Secure Endpoint

Conclusion

Vulnerability management is not a new concept, but due to increased importance, it is high on the priorities list of many organizations' security and risk professionals. This does not only apply to client organizations; many vendors see adding a VM technique as a fair opportunity to evolve their EPP tools. Further, many stand-alone VM tools now offer EPP or EDR functionality to address endpoint security and vulnerability management using a single agent. Security and risk management technical professionals should keep a close track of this evolving space.

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

A Guidance Framework for Developing and Implementing Vulnerability Management

Endpoint Detection and Response: Architecture, Implementation and Operations Practices

The Top 5 Elements of Effective Vulnerability Management

Table 1: High-Level Comparison of Vulnerability Management Tools

Features	Stand-Alone VM Tool	EPP Tool With VM Technique
Scope of Coverage	Wide variety of assets, such as endpoints, network devices, Internet of Things (IoT) devices, cloud workloads, container environments, application scanning	Primarily Windows, Mac and Linux, with very limited support for other asset types
Deployment Architecture	Options are available for on-premises, cloud-hosted and hybrid implementations	Most EPP tools with vulnerability management only support cloud-based implementations
Scanning Technique	Agent-based and agentless scanning	Agent-based, with very limited support for network scanning
Vulnerability Signature	Broad signature coverage	Limited vulnerability signature coverage
Vulnerability Management Tool Ecosystem	Generally well supported by third-party tools for remediation, workflow and automated risk-based vulnerability prioritization	Minimal integrations with third-party remediation tools

Source: Gartner (March 2023)

Table 2: Scenario-Based Selection

Scenario	Type of VM (Stand-Alone Tool or EPP With VM Technique)
You have no VM program in place and need to implement one — often resulting from compliance and regulatory reasons — but your EPP tool offers VM as a technique	Start with the VM technique in EPP, if that feature is available in your platform
You need to assess vulnerabilities on the broadest possible set of operating systems and devices	Prefer a stand-alone VM tool
You need a single consolidated view for application scanning and infrastructure vulnerability scanning	Prefer a stand-alone VM tool
Endpoints are already overwhelmed with a lot of agents	Opt for an EPP tool with a VM technique, or a stand-alone VM tool that supports agentless network scanning
You need third-party VM tool support — that is, prioritization, remediation, workflow	Prefer a stand-alone VM tool

Source: Gartner (March 2023)

Actionable, objective insight

Position your IT organization for success. Explore these additional complimentary resources and tools for technical professionals:

Resource Center

Gartner for Technical Professionals

Explore insights, advice and tools to help technical professionals addres their top challenges.

Learn More

Research

The Future of Cloud Computing in 2027: From Technology to Business Innovation

Uncover the rationale behind these predictions and strategic actions to take.

Download Research

Article

10 Strategic Data and Analytics Predictions Through 2028

Use them in your strategic vision and delivery planning.

Read More

Research

Solution Path for Building Modern Analytics and BI Architectures

Build self-service analytics and business intelligence architectures.

Download Research

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/it

Stay connected to the latest insights

Attend a Gartner conference
View Conference

Gartner®